Konfigurieren von NetFlow/IPFIX für Telemetry Ingest auf SNA

Inhalt

Einleitung

In diesem Dokument werden die Best Practices und die grundlegende Konfiguration von Netflow/IPFIX beschrieben, die Secure Network Analytics (SNA) für die Telemetrie-Erfassung benötigt.

Voraussetzungen

- Kenntnisse über Cisco SNA
- NetFlow/IPFIX-Kenntnisse

Anforderungen

- Sichere Netzwerkanalysen ab Version 7.2.1
- FlowCollector in Version 7.2.1 oder höher
- CLI-Zugriff als Root auf Flow Collector

Verwendete Komponenten

- Dies hängt vollständig von Ihrem Netzwerkdesign und den Geräten ab, die Sie ausgewählt haben, um NetFlow/IPFIX an Secure Network Analytics zu senden. Die NetFlow/IPFIX-Konfiguration unterscheidet sich je nach Exporteur. Für eine detaillierte Konfiguration wenden Sie sich bitte an das Support-Team jedes Exporteurs.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

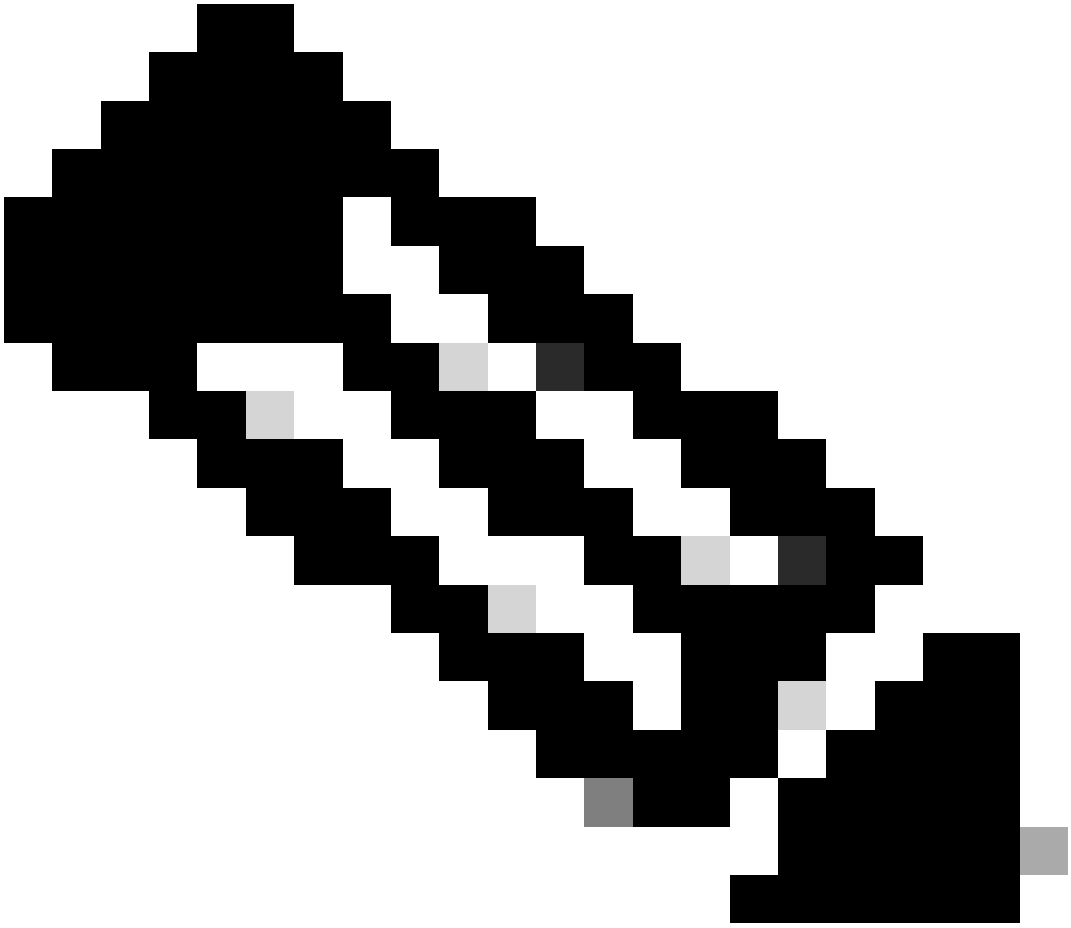
Flow Collector ist eine SNA-Appliance, die für das Erfassen, Verarbeiten und Speichern von Flows zuständig ist, die an Secure Network Analytics gesendet werden. Für NetFlow-Version 9 oder IPFIX können mehrere Felder in der NetFlow/IPFIX-Vorlage enthalten sein, um weitere Informationen zum Netzwerkverkehr hinzuzufügen. Es gibt jedoch neun spezifische Felder, die in der NetFlow/IPFIX-Vorlage enthalten sein müssen, damit Flow Collector diese Flows verarbeiten kann. Flow Collector verarbeitet keine eingehenden Datenflüsse, die eine ungültige Vorlage enthalten. Aus diesem Grund zeigt SNA keine Datenflussinformationen dieser Exporteure unter Web UI oder Desktop Client an.

Konfigurieren

Pflichtfelder

Die nächsten Felder müssen in der NetFlow/IPFIX-Vorlage für die Telemetrie-Erfassung enthalten sein. Stellen Sie sicher, dass diese 9 Felder in der NetFlow/IPFIX-Vorlage enthalten sind, damit Secure Network Analytics eingehende Datenflüsse verarbeiten kann.

- IP-Quelladresse
- Ziel-IP-Adresse
- Quellport
- Zielport
- Layer-3-Protokoll
- Byte Anzahl
- Paketanzahl
- Flow-Startzeit
- Flow-Endzeit



Hinweis: Die NetFlow/IPFIX-Konfiguration könnte weitere Felder enthalten. Die vorherigen Felder stellen jedoch die Mindestanforderungen für Secure Network Analytics für Telemetry Ingest dar.

Empfohlene Felder

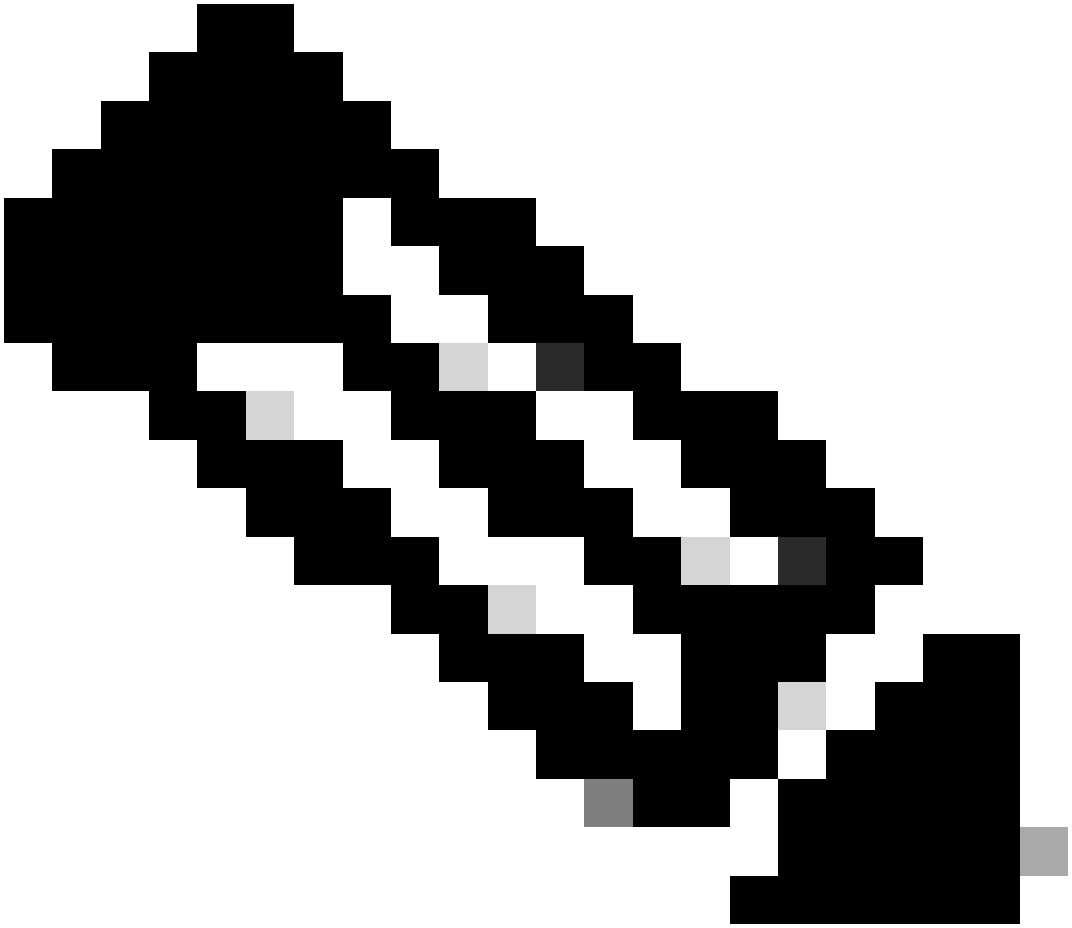
Es wird empfohlen, die nächsten Felder in der NetFlow/IPFIX-Vorlage einzuschließen, um Informationen zu Schnittstelleninformationen zu sammeln. Diese Konfiguration ist erforderlich, um Schnittstelleninformationen wie Name und Geschwindigkeit anzuzeigen:

- Schnittstelleneingang
- Schnittstellenausgang

Best Practices

Darüber hinaus werden die nächsten Einstellungen als Best Practices empfohlen, um eine ordnungsgemäße Durchführung von Secure Network Analytics sicherzustellen.

- Aktives Timeout auf 60 Sekunden setzen
- Inaktives Timeout auf 15 Sekunden setzen
- Zeitüberschreitung für Vorlage auf 30 Sekunden festlegen



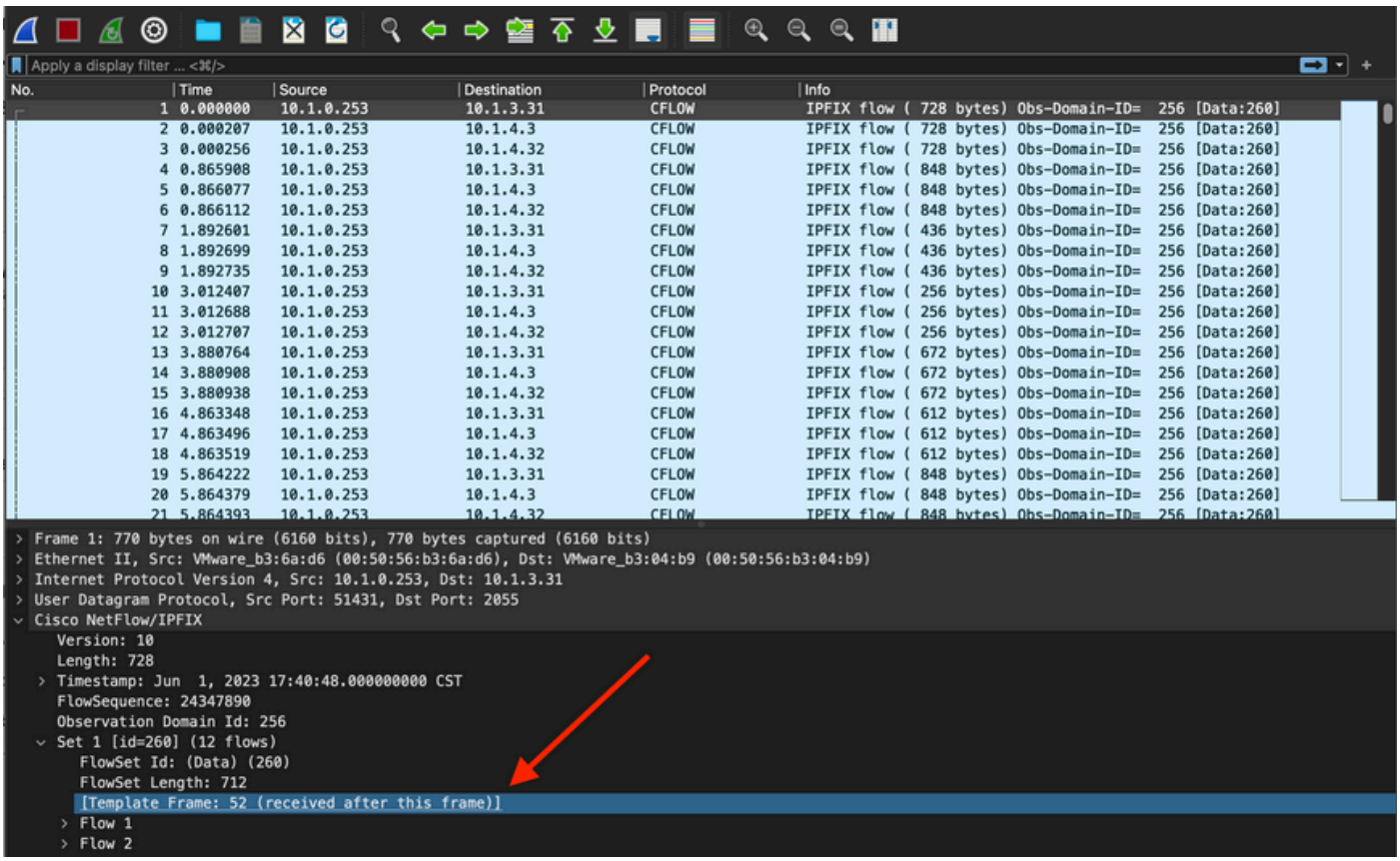
Hinweis: Der Standard-Port für NetFlow ist 2055. Sie können jedoch einen anderen Port auswählen. Stellen Sie sicher, dass derselbe Port während des letzten Prozesses für Flow Collector(s) verwendet wird.

Überprüfung

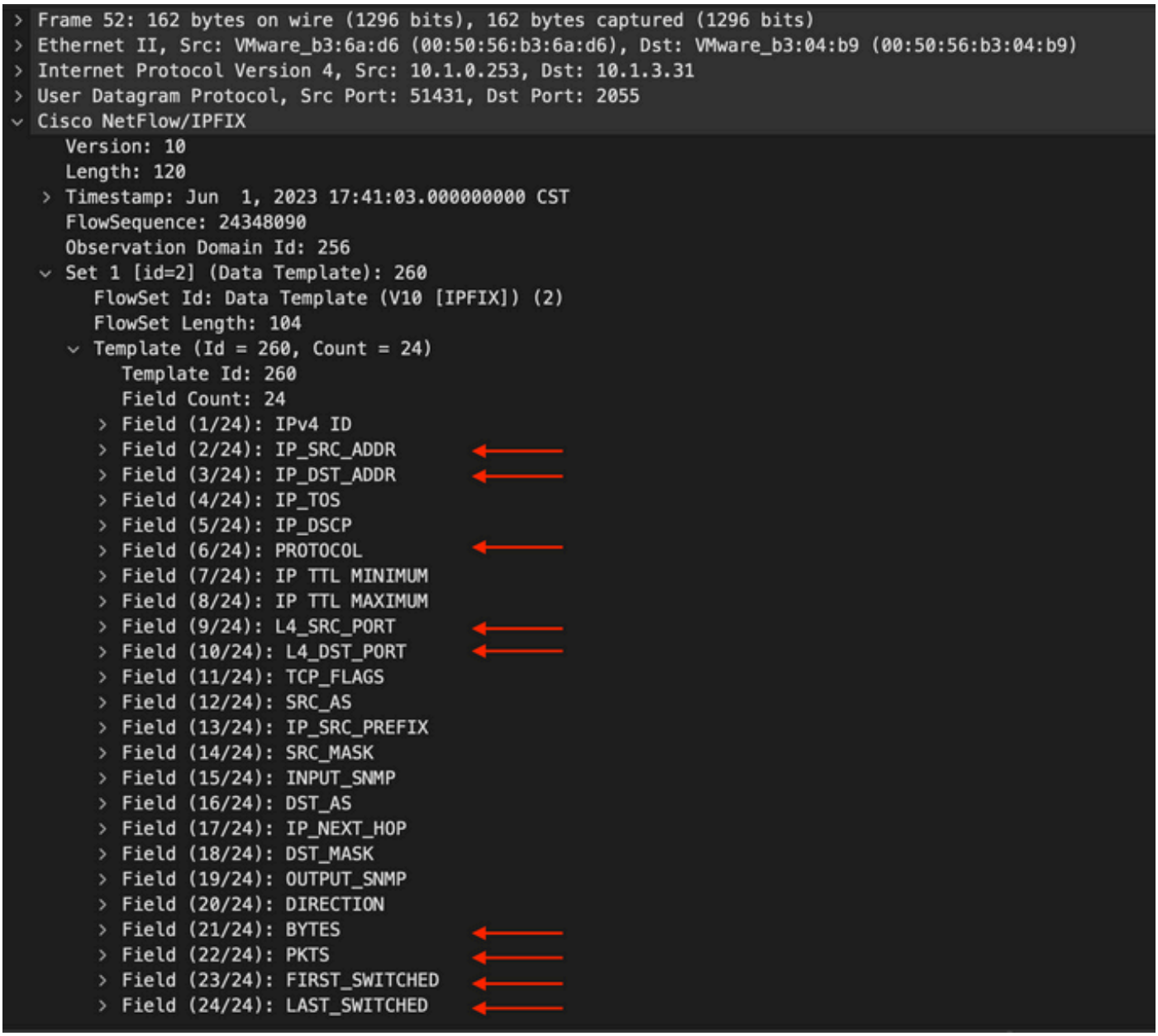
Zur Validierung der NetFlow/IPFIX-Vorlagenkonfiguration können Sie eine Paketerfassung zwischen dem Exporter und FlowCollector ausführen. Melden Sie sich bei Flow Collector mit dem Root-Benutzer über SSH an, und führen Sie den folgenden Befehl aus:

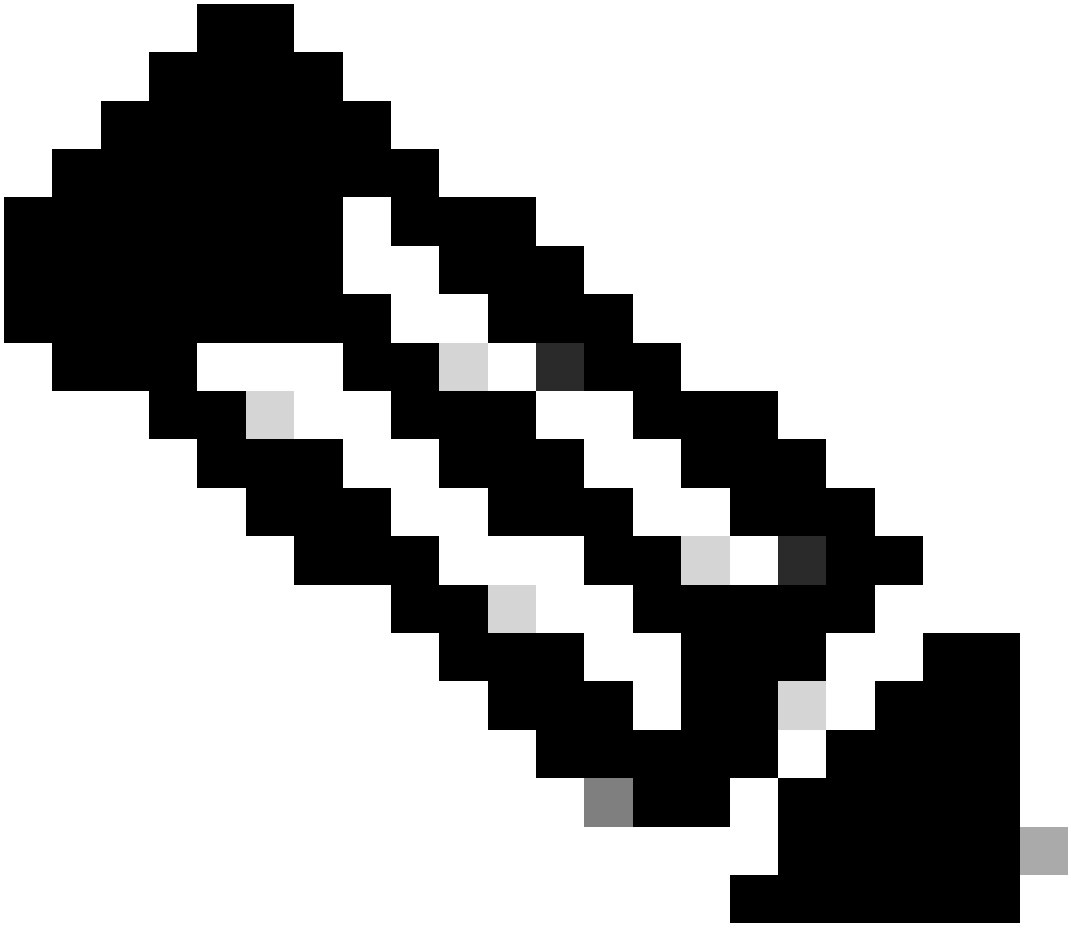
```
tcpdump -nli [Collecting_Interface] host [Exporter_IP_Address] and port [NetFlow_Port] -w /lancope/var/
```

- Verwenden Sie ein SCP-Tool, um die Paketerfassung vom Flow Collector (in /lancope/var/tcpdump) auf Ihren lokalen Computer zu exportieren und dann in Wireshark zu öffnen.



- Identifizieren Sie den Frame, in dem die NetFlow/IPFIX-Vorlage empfangen wurde, und öffnen Sie sie, um die in der Vorlage enthaltenen Felder zu überprüfen.


Frame 52: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: VMware_b3:6a:d6 (00:50:56:b3:6a:d6), Dst: VMware_b3:04:b9 (00:50:56:b3:04:b9)
Internet Protocol Version 4, Src: 10.1.0.253, Dst: 10.1.3.31
User Datagram Protocol, Src Port: 51431, Dst Port: 2055
Cisco NetFlow/IPFIX
Version: 10
Length: 120
Timestamp: Jun 1, 2023 17:41:03.000000000 CST
FlowSequence: 24348090
Observation Domain Id: 256
Set 1 [id=2] (Data Template): 260
FlowSet Id: Data Template (V10 [IPFIX]) (2)
FlowSet Length: 104
Template (Id = 260, Count = 24)
Template Id: 260
Field Count: 24
Field (1/24): IPv4 ID
Field (2/24): IP_SRC_ADDR
Field (3/24): IP_DST_ADDR
Field (4/24): IP_TOS
Field (5/24): IP_DSCP
Field (6/24): PROTOCOL
Field (7/24): IP TTL MINIMUM
Field (8/24): IP TTL MAXIMUM
Field (9/24): L4_SRC_PORT
Field (10/24): L4_DST_PORT
Field (11/24): TCP_FLAGS
Field (12/24): SRC_AS
Field (13/24): IP_SRC_PREFIX
Field (14/24): SRC_MASK
Field (15/24): INPUT_SNMP
Field (16/24): DST_AS
Field (17/24): IP_NEXT_HOP
Field (18/24): DST_MASK
Field (19/24): OUTPUT_SNMP
Field (20/24): DIRECTION
Field (21/24): BYTES
Field (22/24): PKTS
Field (23/24): FIRST_SWITCHED
Field (24/24): LAST_SWITCHED



Hinweis: Die angezeigten Feldnamen können je nach Exporteur unterschiedlich aussehen. Dies ist nur ein Hinweis darauf, wie Sie diese Felder validieren können.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.